GOVERNMENT OF TELANGANA
ABSTRACT

IT,E&C Dept – Cloud Adoption Policy of the Government of Telangana – Orders – Issued.

(INFORMATION TECHNOLOGY, ELECTRONICS & COMMUNICATIONS DEPARTMENT)

G.O.Ms.No. 10 **Dated: 09-10-2020**

Read:

* * *

ORDER:

The following instructions will apply to all Government Departments, Sub-Ordinate offices, Public Sector Undertakings, Urban and Rural Local Bodies & any Body/Organization set up under any law of the State Government (henceforth collectively referred to as "User Departments")

2. Government of Telangana is continuously encouraging and adopting the use of Emerging Technologies for Governance. The State Government understands the potential of cloud technology in transforming service delivery to citizens and is therefore targeting to drive large scale adoption of cloud within all its User Departments.

3. State Data Centres (SDCs), so far have been identified as core infrastructure to support eGovernance initiatives under NeGP. Similarly, Telangana's SDC has been offering hosting, disaster recovery, and other remote management services to many Departments and Corporations in the State. At present, SDC's existing capacity has reached the saturation point.

4. While the SDC has served multiple departments so far, because of the capacity constraints, there are instances in the recent past where SDC has faced challenges in scaling up and meeting the user department requirements in a timely fashion leading to application downtimes and poor user experience. This was even more prevalent when such load spikes cannot be anticipated ahead of time.

5. In view of the above and also taking cognizance of the Meghraj Policy announced by Government of India, the advent of advanced and affordable cloud services, and the high costs of refreshing the hardware at the data centres – the Government is **mandating all departments to deploy their existing** (under the scenarios mentioned in Point No.6) **or new applications on Cloud except Top Secret and Secret** (data or information that can cause serious damage to the security of the state/country or to the state/national interests)**.** The Top Secret and Secret applications can continue to be hosted in their existing set ups or facilities (SDC/Dedicated Environments).

6. A few indicative scenarios/opportunities (not exhaustive), to move to cloud are when:

- The existing ICT infrastructure is nearing contract expiry
- Refresh or Upgrading of existing applications or ICT infrastructure is required.
- Capacity enhancement is required due to issues of resiliency and/or performance,
- Evaluating options to lower the Total Cost of Ownership (TCO).
- Procuring new applications or ICT infrastructure

7. However, if a department intends to seek an exemption from G.O.Ms.No. Because of some inherent benefits of on-premise ICT infrastructure, or some challenges in moving to cloud, then the User Department can make an **exemption request** submitting the proposal along with justification for seeking the exemption. The committee headed by the Principal Secretary, ITE&C and comprising of cloud specialists and officials shall evaluate the exemption request and communicate the decision (approve or reject) on the exemption request within two weeks from the receipt of the request from the departments.

8. The State, via its Cloud First policy, aims to enable the acceleration of eGovernance plans, transform the speed, scale and quality of citizen service delivery's, achieve low cost, high operational efficiency, and also emerge as a leader of Emerging Technologies in India.

9. Cloud adoption will provide the users with high elasticity, visibility and control over their workloads, with billing or payments being solely based on consumption. A broad range of services can be unlocked to optimize costs, performance, security, and realize benefits such as consumption-based pricing (pay-as-you-go model). The enclosed "Cloud Adoption Framework" **enclosed with the policy** details out the required knowledge and procurement principles for cloud adoption in User Departments.

(Contd. Pg: 2)

10. MeitY has empanelled Cloud Service Providers (CSPs). Cloud services must be procured from these technically empanelled CSPs or their authorised partners. Empanelled CSPs are audited by Standardisation Testing and Quality Certification (STQC) and can be found at https://www.meity.gov.in/content/gi-cloud-meghraj\

11. User Departments can also leverage their existing procurement processes, and/or cloud services listed on GeM (https://mkp.gem.gov.in/services#!/browse/) to start procuring cloud and managed services from the CSP or their authorized partners.

12. In order to facilitate and simplify the procurement process and accelerate the cloud adoption, a catalogue of CSP's services along with their discovered prices, would be made available on the e-procurement portal of Telangana State Technology Services (TSTS).

13. Going forward, ITE&C Department will minimize further investments in expanding the infrastructure in SDC and will only maintain the existing capacity. Eventually the SDC users will have to move to cloud.

14. Currently, many User Departments are procuring and maintaining their own physical ICT infrastructure (servers, storage, firewalls, routers etc) at their own cost. Similarly, **all costs towards adoption of cloud - moving the existing or procurement of new applications- shall be borne by the respective departments.** However, ITE&C Department will offer the necessary support to all the departments in their cloud journey.

(BY ORDER AND IN THE NAME OF THE GOVERNOR OF TELANGANA)

JAYESH RANJAN
PRINCIPAL SECRETARY TO GOVERNMENT

To
All the Departments of Secretariat
The Metropolitan Commissioner, HMDA, Hyderabad
The Commissioner, Greater Hyderabad Municipal Corporation, Hyderabad
The Commissioner and I.G., Stamps and Registration, Hyderabad
The Vice Chairman and Managing Director, TSIIC, Hyderabad
The Commissioner of Industries, Hyderabad
The Commissioner, Information and Public Relations, Hyderabad
The Member Secretary, TS Pollution Control Board, Hyderabad
The Chairman & MD, TSTRANSCO, Hyderabad
The Chairman & MD, TSSPDCL/TSNPDCL/ TNREDCL
The Commissioner of Labour, Hyderabad
The Development Commissioner, VSEZ, Hyderabad
The Director, STPI, Hyderabad
The President, HYSEA, Hyderabad
The Regional Director, NASSCOM, Hyderabad
The CEO, T-Hub, Hyderabad
The President, FTAPCCI, Hyderabad
All the District Collectors

Copy to:

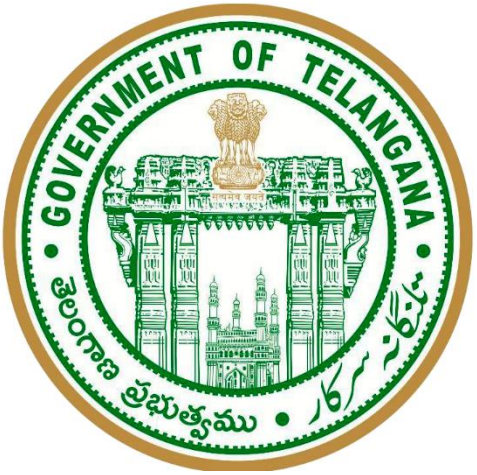
The Secretary to GoI, DIPP, Ministry of Commerce & Industry, GoI, New Delhi
The Hon'ble Chief Minister's Office/PRO to C.M.
The PS to Hon'ble Minister for IT, MA&UD, Industries,
Hyderabad. The PS to Hon'ble Minister for Finance, Hyderabad
The PS to Hon'ble Minister for Revenue, Hyderabad.
The PS to Hon'ble Minister for Energy, Hyderabad.
The PS to Hon'ble Minister for Labour, Hyderabad.
The PS to Chief Secretary

SF/SC

// FORWARDED: : BY ORDER //

SECTION OFFICER

Telangana State
Cloud Adoption Framework



ITE&C Department, Govt of Telangana

September 2020

Contents

1. Introduction: Cloud Adoption Framework 3

2. Pillar A: Telangana's Cloud Mandate 3

3. Pillar B: Understanding Cloud 5

3.1. Cloud Adoption in Government 5

3.2. What is Cloud? 7

3.3. Security in Cloud 10

3.4. Cloud Cost Analysis 12

4. Pillar C: Plan and Procure 13

4.1. Cloud adoption plan 13

4.2. Re-thinking Procurement to extract cloud benefits 13

4.3. Governance and Continuous Optimization 21

5. Pillar D: Cloud Adoption Support 21

5.1. Cloud Centre of Excellence 22

5.2. Catalogue of CSP services 22

1. Introduction: Cloud Adoption Framework

Objective: This document aims to help enable state government departments to understand Telangana's cloud mandate [G.O.Ms.No.10] and impart the know-how required to comply with the said mandate.

To its intended audience, the contents of this document are written in a way to empower the reader with the required knowledge and tools to adopt Telangana's cloud mandate. It gives a crisp walk-through for the same via the below-mentioned Cloud Adoption Framework:

Cloud Adoption Framework

Pillar A	Pillar B	Pillar C	Pillar D
Telangana's Cloud mandate	**Understanding Cloud**	**Planning and Procurement**	**Cloud Adoption Support**
✓ Government Order	✓ Adoption in Government	✓ Cloud Adoption Plan	✓ Cloud Centre of Excellence
✓ Stata Data Centre	✓ What is Cloud?	✓ Rethink procurement to extract cloud benefits • Budgeting • Requirements • Scope of Work • Evaluating as service • Commercial Evaluation • Contracting	✓ Catalogue of CSP services
✓ Opportunities for immediate migration	✓ Key benefits of cloud		
	✓ Security in Cloud		
	✓ Cloud Cost Analysis		
		✓ Governance and Continuous Optimization	

2. Pillar A: Telangana's Cloud Mandate

Year after year, Telangana has been adjudged as the leading e-governed state in India. What sets Telangana apart from its peers is the vision of a truly digital Telangana and its execution by the leadership. Telangana is continuously encouraging and adopting the use of emerging technologies for governance. The state government understands the potential of cloud technology and is targeting to drive large scale adoption of cloud within all its departments. This policy is an endeavour in this direction.

State Data Centres (SDCs), earlier had been identified as core infrastructure to support e-Governance initiatives under NeGP. In line with that, Telangana's SDC was established in 2011. The phase-II expansion of SDC's infrastructure was discontinued after the bifurcation of erstwhile united AP in 2014. It has been offering hosting, disaster recovery, and other remote management services to many departments and corporations in the state. At present, SDC's existing capacity has reached the saturation point.

While the SDC has served multiple departments so far, because of the capacity constraints, there are instances in the recent past (mentioned below) where SDC has faced challenges in scaling up and meeting the user department requirements in a timely fashion leading to application downtimes and poor user experience. This was even more prevalent when such load spikes cannot be anticipated ahead of time.

- **Streenidhi project:** (Credit Cooperative) faces seasonal load of collections and reconciliations every year in March. System faces downtime during these periods as the database server goes into high utilization. SDC is not able to allocate any additional cores as it is deployed on a shared capacity and any reallocation of cores will affect the other applications deployed on the same cluster. SDC is also unable to expand the overall cluster capacity because of budget issues. Even if it were to expand the capacity and allocate additional cores to Streenidhi project, the capacity will remain idle / underutilized throughout the year except for reconciliation period.
- **MGNREGA:** Currently facing performance issues as the Oracle Exadata, on which the application is deployed, has reached maximum capacity. The department has to either procure additional capacity or upgrade the database to a latest version and deploy on a separate rack. Either of the tasks are time consuming resulting in continuing performance issues for the end users.
- **Dharani Project:** Application became quite slow because of the large database size. SDC was not able to provision additional capacity to meet the requirement. Later, the department procured the physical servers and deployed in SDC to adequately meet the demand.
- **HMWSSB & IGRS:** Currently facing performance issues as the Oracle ExaData, on which the application is deployed, has reached maximum capacity. The department has to either procure additional capacity or deploy on a separate ExaData Box. Either of the tasks are time consuming resulting in continuing performance issues for the end users.

In view of the above and taking cognizance of the Meghraj Policy announced by Government of India, the advent of advanced and affordable cloud services, and the high costs of refreshing the hardware at the data centres – the government is **mandating all departments to deploy their existing or new applications on cloud except Top Secret and Secret** (data or information that can cause serious damage to the security of the state/country or to the state/national interests) for the following indicative opportunities (non-exhaustive):

- The existing ICT infrastructure is nearing contract expiry
- Refresh or Upgrading of existing applications or ICT infrastructure is required.
- Capacity enhancement is required due to issues of resiliency and/or performance,
- Evaluating options to lower the Total Cost of Ownership (TCO).
- Procuring new applications or ICT infrastructure

The Top Secret and Secret applications can continue to be hosted in their existing set ups or facilities (SDC/Dedicated Environments). The departments shall consider Public Cloud/Virtual Private Cloud to deploy the applications.

However, if a department intends to seek an exemption from [G.O.Ms.No.10] because of some inherent benefits of on-premise ICT infrastructure, or some challenges in moving to cloud, then the user department can make an **exemption request** submitting the proposal along with justification for seeking the exemption.

The state, via its Cloud First policy mandate, aims to enable the adoption and acceleration of e-governance plans, transform the speed, scale and quality of citizen service delivery, achieve low cost, high operational efficiency, and also emerge and act as a leader of Emerging Technologies in India.

Cloud adoption will provide the users with high elasticity, visibility and control over their workloads as well as billing based solely on corresponding consumption. A broad range of services can be unlocked to optimize costs, performance, security, and many more benefits as discussed in the next sections.

MeitY has technically empaneled Cloud Service Providers (CSPs). Services must be procured from these CSPs or their authorised partners. The departments can also leverage their existing processes, and/or cloud services listed on GeM(https://mkp.gem.gov.in/services#!/browse/) to start procuring cloud.

To further simplify the procurement process and accelerate cloud adoption, a catalogue of CSP's services along with their discovered prices, would be made available on the e-procurement portal of Telangana State Technology Services (TSTS).

Going forward, ITE&C Department will minimize all physical infrastructure investments in SDC. And eventually all the SDC users will be moved to cloud.

Currently, many user departments are procuring and maintaining their own physical ICT infrastructure (servers, storage, firewalls, routers etc) at their own cost. **Similarly, all costs towards adoption of cloud - moving the existing or procurement of new applications - shall be borne by the respective departments.** However, ITE&C Department will offer the necessary support to all the departments in their cloud journey

3. Pillar B: Understanding Cloud

3.1. Cloud Adoption in Government

Keeping pace with advances in technology, Ministry of Electronics and Information Technology (MeitY), Government of India had announced the *MeghRaj Policy* (GI Cloud Initiative) in 2013. The policy provides strategic direction for adoption of cloud services at all levels of Indian Government. It was developed with the targets of improving scale and quality of citizen service as well as to optimize the IT expenditure.

MeitY had started *technical*[1] *empanelment of cloud service providers* in 2016 so that no level of Indian government has to expend any time and resources in having to do their individual assessment of the CSPs on the various compliance, security and legal / regulatory requirements.

Empanelled CSPs were audited by STQC[2] and can be found at https://www.meity.gov.in/content/gi-cloud-meghraj. The list gets updated regularly.

[1] **Technical Empanelment:** In case of a successful audit of Data Center(s) and Cloud Service Offerings by STQC, MeitY issues a Letter of Empanelment to the CSP clearly mentioning the Cloud Service Offerings and Cloud Deployment Models. Not to be confused with price empanelment.
[2] **STQC:** Standardisation Testing and Quality Certification

Their cloud services along with pricing, are listed (directly or via their partners) on Government e-Marketplace (https://mkp.gem.gov.in/services#!/browse/) under MeitY's empanelled Basic and Advanced cloud services categories. The departments can float a Request for Quotation (RFQ) on the portal to select a CSP or its authorised partner.

Over the last few years, multiple international and national governments have come to successfully embrace cloud technologies.

Global Trends	Countries like UK, Singapore, US, Canada, Australia, Philippines and the European Union have published their policies for cloud adoption within government.
Indian Government Bodies	Ministry of Civil Aviation, Ministry of Agriculture, Ministry of Human Resource Development | IRCTC, GSTN, CPWD, NHAI, NTPC, AICTE, SEBI, MECL, AAI | Maharashtra, Kerala, Karnataka, Punjab, Assam
Other States	**Maharashtra:** Mahaonline – Farmer Loan Waiver Scheme, Direct Benefit Transfer (DBT), Tourism, Skills, Water Resource departments etc. **Punjab:** Workloads of Directorate of Governance Reforms (DGR) etc. **West Bengal:** Blockchain-enabled birth and death registration application etc. **Assam:** NRC Portal, **AICTE:** Digital Learning Platform, **SEBI:** Big Data solution using HDFS, Document Management System, mail and messaging, SEBI Website, Investor Portal etc. **MECL:** DR on cloud for SAP, **AAI:** e-Boarding, **MHRD:** Swayam Project

Telangana State	• Portals, ERP applications such as ones belonging to GHMC, KMC
	• Emerging Technologies:
	  • T-Chits, an award winning blockchain-based application for managing Chit Fund businesses across the state runs on cloud;
	  • Pensioner's Life Certificate through Selfie, is an example of AI-based facial recognition and comparison, developed using platform services of cloud.
	  • Road Transport Authority FEST (Friendly Electronic Services of Transport) also uses AI-based facial recognition and comparison, developed using platform services of cloud.
	  • DOST(Degree Online Services Telangana) also uses AI-based facial recognition and comparison, developed using platform services of cloud.
	  • Many PoCs based on emerging technologies are being quickly developed, tested and deployed in cloud environments.

3.2. What is Cloud?

Cloud computing has been defined by NIST (National Institute of Standards and Technology, USA) as a model for enabling convenient, on-demand[3] network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or cloud provider interaction.

Put simply, cloud computing provides a variety of computing resources and services over a network. These services can be remotely accessed and utilized by multiple users of the department on-demand, without the risks of hardware failure.

Cloud Services, as identified by MeitY[4]		
	Basic Cloud Services	**Advanced Cloud Services**
Compute Services	Virtual Machine	Containers[5]
Storage Services	Block, Object, File, Archival	-
Database	Managed Database as a Service	-
Network Services	Load Balancer[6], VPN Gateway, Firewall, Public IP	Content Delivery Network, MPLS Connectivity
Security Services	Identity and Access Management	Hardware Security Module[7], Distributed Denial of services, TLS/SSLCertifcate Management, Multi-factor authentication.
Other Services	-	Monitoring (Log Analysis, Operational Metric Collection, Alarm Service, Notification Service) Office Productivity Suite Analytics Services (Video/Data Streaming, Big Data, Data Warehousing[8]),

Cloud Service Providers (**CSPs**) are companies which offer cloud as a service.

[3] Need-basis
[4] Cloud services bouquet – from invitation for empanelment of cloud service providers (2020)
[5] **Containers** are the lightweight alternatives to Virtual Machines. Containers allow to encapsulate an application's code, libraries, configuration and other dependent files into one single package (MeitY Cloud Services Bouquet, 2020)
[6] **Load balancing** refers to evenly distributing load (incoming network traffic) across a group of backend resources or servers.
[7] **HSM**: A hardware security module (HSM) is a physical computing device that safeguards and manages digital keys, performs encryption and decryption functions for digital signatures, strong authentication and other cryptographic functions
[8] **Data Warehousing:** A central repository of information which acts as a single source of truth and which can be used to generate variety of reports and dashboards to assist in the decision making process.

Managed Service Providers (**MSPs**) are companies which provide handholding support to the government departments in migrating to cloud.

Key benefits obtained from adopting Cloud Computing:

Zero capex and consumption-based pricing	Unlike traditional IT hardware, there is no need to invest in inflexible infrastructure which lies heavily underutilized[9] (due to "peak load" procurement) and entails high maintenance costs. Department only pays for the services consumed which can be availed on-demand.
As-a-service Model vs Fixed Infrastructure	In traditional deployments, the entire infrastructure for the total project period is procured and commissioned for each project. With cloud, it is no longer required to procure the entire infrastructure, but you can start with minimum requirements and can scale-up as the demand goes up. Also the departments do not have to be concerned with periodical replace/refurbish of hardware. CSPs own the onus of capacity planning, augmentation, maintenance, and hardware refresh.
Simple to define and Manage SLAs	Traditional SLAs are hard to define, trace and enforce. CSPs offer standard publicly available commercial SLAs (e.g., uptime, durability) for their cloud services.
Remarkably simple cloud vendor change	The transition at the end of the contract period is seamless, as it involves only migrating the applications and data from one CSP to the other, using the tools available with the CSP or third party.
No need to buy separate proprietary licenses and services	With cloud, departments can save licensing costs as they will no longer need to procure licenses or additional support separately on a capex basis. CSPs offer options with multiple open source operating systems (e.g., Open Linux), open source databases (e.g., PostgreSQL, MySQL, MariaDB) as well as commercial operating systems (e.g., Windows, RHEL) and databases (e.g., MS SQL, Oracle) on Opex basis.
Variety of Cloud Services	Departments can provision a variety of compute resources, add / modify virtual machines, augment storage allocation, and change security configuration during the course of the project as per their requirements unilaterally without requiring human interaction with each service provider.
Agility	The self-service and on-demand nature of the cloud services provides agility. The department can start with smaller and lower specifications in cloud, auto-scale or right-size (lower end to higher specifications or vice versa), provision large number of compute instances for a short duration (e.g., load testing) turn-off

[9] A 2017 Study by IDC stated that typical data centers are 45% utilized.*

<table>
<tr><td></td><td>environments (e.g., pre-production) when not required, add additional storage capacity with zero lead times to deliver consistent performance service levels at optimal cost. All these benefits can be availed with the click of a button.</td></tr>
<tr><td>Optimize storage costs based on use case</td><td>Departments will have multiple choices in selecting storage services. The variety of storage options in cloud gives the Departments the ability to use the appropriate storage based on the use case optimizing the overall project cost as compared to a traditional on-premises environment. For example:
<table>
<tr><td>High IOPS SSD</td><td>For latency[10] sensitive applications</td></tr>
<tr><td>SSD</td><td>For low latency requirements</td></tr>
<tr><td>HDD</td><td>For throughput[11] intensive / less frequently accessed workloads</td></tr>
<tr><td>Magnetic Disks</td><td>For infrequent data access</td></tr>
<tr><td>Object Storage</td><td>For unstructured data</td></tr>
<tr><td>Cold Storage</td><td>For archival data</td></tr>
</table></td></tr>
<tr><td>Advanced Services</td><td>Some CSPs offer advanced services such as serverless, analytics, application services, deployment, management, IoT, AI, machine learning, blockchain etc. Departments can leverage these on a pay-as-you-go basis to develop innovative citizen services. The ease of access to these services with no upfront costs enables Departments to experiment boldly, conduct faster proof of concept validations, and arrive at a desired launchable solution form.</td></tr>
</table>

Given such benefits of moving to cloud, all popular and hyper-scale IT products today run on cloud, including - Youtube, Whatsapp, Facebook, Twitter, Instagram, Netflix, Gmail, LinkedIn, Amazon, Skype.

<u>Cloud Service Models for consumption:</u>

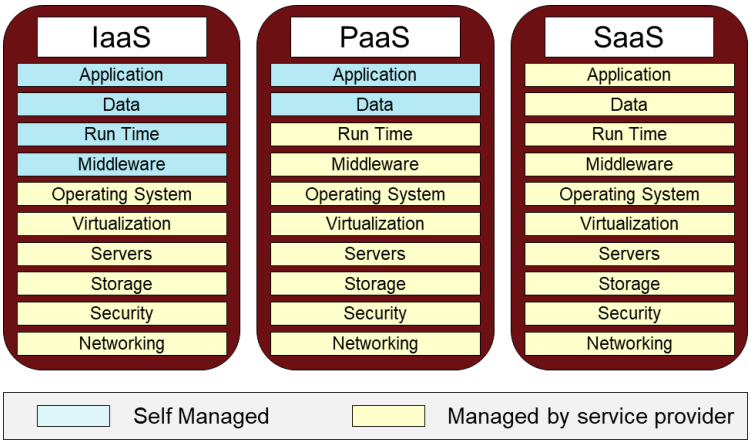
Cloud computing has multiple service models. The standard models are: Infrastructure as a Service (**IaaS**), Platform as a Service (**PaaS**) and Software as a Service (**SaaS**).

IaaS model: Department can choose to utilize only the virtual machines, storage services (IaaS) from the CSP and deploy/manage their own application or database software

PaaS model: They may also opt for taking platform services (e.g., database, containers, developer tools, AI/ML suite) where the application/database software including the underlying Virtual Machines is managed by the CSP.

[10] **Latency** is the delay between a user's action and a web application's response to that action.
[11] **Throughput** is the rate of data transfer.

SaaS model: In a few use cases, where available, the department may take the entire software as a service (referred as SaaS) without having to invest on the application development, middleware licenses and underlying infrastructure. The mix of the above models for an application typically depends on the application (e.g., granularity of control) and business (e.g., need for ease of management) requirements.



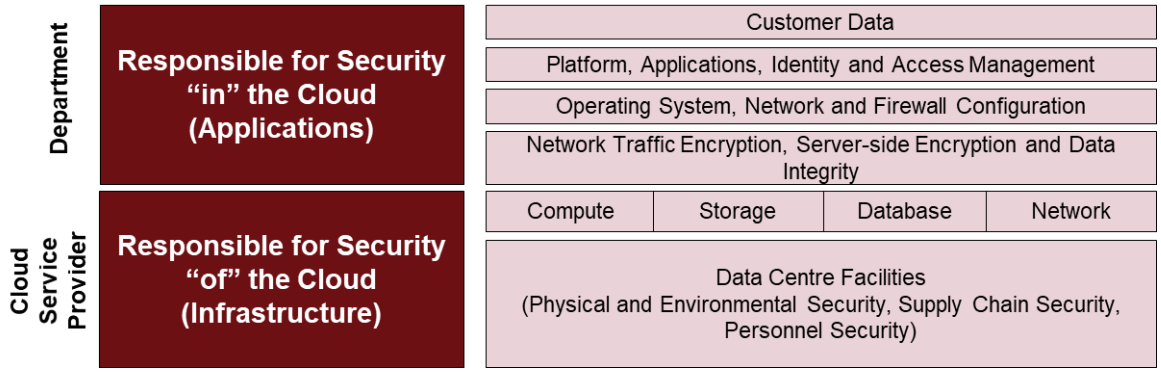
3.3. Security in Cloud

Typically Cloud Service Providers make sizeable investments in cyber defense research and development, while employing thousands of security experts who are pre-empting and resolving potential threats on a daily basis. This makes their security function much more robust than most in-house teams across public and private sector.

Shared Responsibility Model

Security is a shared responsibility between the departments and the CSP. The cloud model redefines and simplifies the roles that departments and their vendors need to carry out.

Cloud Service Providers (CSPs) take responsibility of the infrastructure that is under their control and implement a variety of controls, ensuring *security "of" the cloud. They* are responsible for operating, managing, and controlling the components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate.



A variety of security controls are put in place by the CSPs.

Traditional standards / controls: CSPs implement **ISO 27001** controls (e.g., *Datacentre Physical Security & Environmental Controls, Supply Chain Security, Personnel Security, Network Security)* and

Cloud specific standards / controls: **ISO 27017** guidelines for information security controls applicable to the provision and use of cloud services; **ISO 27018** guidelines that establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in line with the privacy principles in **ISO/IEC 29100** for the public cloud computing environment;

CSPs offer assurances of effective physical and logical security controls through the third-party certifications. All the empanelled CSPs are audited by STQC. As per MeitY Empanelment guidelines and the STQC audit requirements, the third-party certification for **ISO 27001**, **ISO 27017**, and **ISO 27018** are mandatory.

Other key security features available:

- **Logical Isolation** of virtual machines, network and storage in a cloud environment offers a secure multi-tenant environment to ensure separation between different consumers of the service to prevent one malicious or compromised consumer from affecting the service or data of another.

- **Secure Data Erasure** is available in cloud once the Department deletes the data.

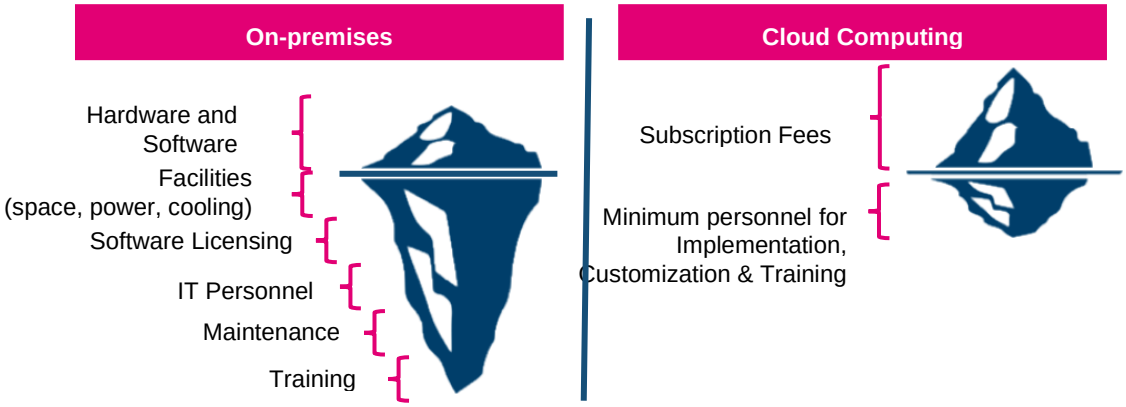
- ***In-built security services:*** While CSPs are responsible for securing the infrastructure, they offer a suite of comprehensive security, management and monitoring services that enable departments to have complete visibility and control on management of the guest operating system (including updates and security patches), other associated application software, and content hosted in cloud as well as configuration of the suite of cloud security services (e.g., Firewall, Encryption, HSM) to secure the applications as they would in a traditional on-premises environment.

- ***Third-party security tools:*** Departments can also implement additional third-party security tools (e.g., Data Leak Protection, Next Generation Firewall, Advanced Threat Analytics, Vulnerability & Penetration Testing) to complement and enhance Departments' operations in the Cloud. These products complement existing CSP's Cloud services to enable Departments to deploy a comprehensive security architecture as they would in a traditional on-premises environment. The departments based on the application's requirements can choose the security controls or services to safeguard the application and data.

3.4. Cloud Cost Analysis

Understanding cost benefits (acquisition and operating costs) of cloud computing is critical for decision making. Total Cost of Ownership (TCO) analysis is used for comparing the costs of running workloads on premises (or in a co-location facility) versus on cloud. *A 2017 Study by IDC stated that typically only 45% of the data centre's capacity is utilized*[12]*, making 55% of the capacity idle or redundant.*

Cloud becomes economical when considering all the cost elements that make up the on-premises environment. On the other hand, cloud gives the ability of starting small and scaling-up as required in cloud.



- **On-Premises Environment**: Ensure inclusion of initial capex and annual maintenance costs of:
    - Servers (e.g., Server, Rack Chassis PDUs, ToR Switches)
    - Storage (e.g., Storage Disks, SAN/FC Switches)
    - Network (e.g., LAN Switches, Load Balancer Bandwidth costs)
    - Software (e.g., OS, Virtualization s/w Licenses, backup s/w)
    - Security (e.g., firewalls, DDOS, encryption, identity and access management)
    - Monitoring (e.g., utilization monitoring, network monitoring)
    - IT Manpower Costs (e.g., Server Admin, Virtualization Admin, Storage Admin, Network Admin, Support Team)
    - Facilities[13] (e.g., space, power, specialized air conditioning)

- **Cloud Environment:** Cost calculation should factor for:
    - Ability to start with smaller configuration and change configuration on-demand
    - Storage optimization
    - Mix of multiple pricing models (e.g., on-demand, committed).

[12] IDC White Paper, sponsored by Hewlett Packard Enterprise, Quantifying Datacenter Inefficiency: Making the Case for Composable Infrastructure, Published March 2017. This is measured in terms of the amount of idle compute hours and unused storage capacity for provisioned components.
[13] In case of a co-located environment, the co-located provider charges for facilities costs on the basis of the number of racks to be deployed

4. Pillar C: Plan and Procure

4.1. Cloud adoption plan

The following high-level policy guidance helps departments to choose the right workloads to get started with cloud adoption:

1. Look at **development and test** workloads as a learning path to cloud adoption.
2. Use cloud for **entirely new applications**. Building new applications on the cloud provides all the advantages of cloud right from the get-go.
3. As cloud skills and maturity develops, look to **migrating websites** and digital properties, analytics, and mobile applications to the cloud.
4. Move **mission-critical applications** to the cloud and ensure that the cloud is leveraged for its enhanced Disaster Recovery capabilities.
5. **Migrate entire on-premise data centers** to the cloud and go **'all-in.**' Thinking long term, cloud adoption plans should consider whether there will be a need for data centers that are coming up for lease in 6/12/18 months, or others that will require a significant technology refresh? Can these workloads be moved to, or built on, the cloud instead?

Most traditional applications, including applications running in a virtualized environment (e.g., VMWare, HyperV, KVM) can be migrated (lift-and-shift) to cloud without the need for any changes to the applications.

It is important to plan your migration to coincide with hardware retirement, license and maintenance expiration, and other frugal opportunities to realize cost savings.

4.2. Re-thinking Procurement to extract cloud benefits

Once the decision to adopt cloud has been made, obtaining cloud services to adequately meet project goals is critically dependent on procurement. A shift to the cloud is a departure from traditional procurement processes, which are not structured to acquire services. It is also a shift from a fixed-cost model to a consumption-based pricing model.

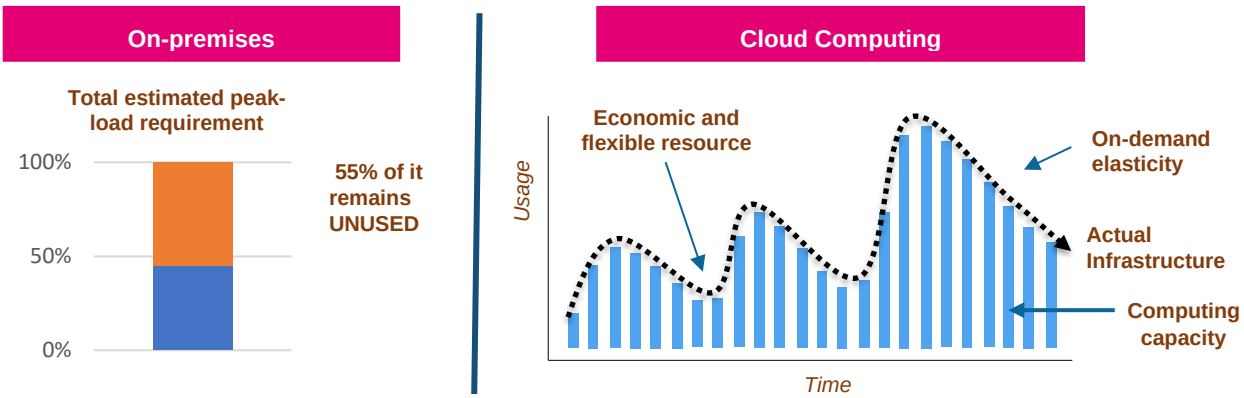
Traditional procurement and contracting processes when applied to cloud, can inflate costs, limit cloud capabilities and delay cloud-enabled transformation.

Therefore, procurement officials should re-think their own approach while adopting cloud, and re-engineer their internal mechanisms to create flexible procurement processes leveraging cloud's *Agility, Elasticity and Multiple Pricing Models.*

The following sections walk you through how each traditional procurement and contracting steps must be re-thought:

1. Re-thinking Budgeting

Traditionally, IT budgeting is built around estimating and buying for "peak load" requirements because of inflexible infrastructure and long procurement lead times. Budgeting considers the first year CapEx investment requirement followed by annual recurring expenditure (e.g., AMC/ATC for hardware and software).



Re-thinking Budgeting: *On-premises vs Cloud Infrastructure*

In Cloud, the department should carry out an **Opex-based budgeting**, where the capacity & cost estimation is done based on the expected usage in a given month or a quarter based on the nature of the workload (e.g., spiky, part-time, cyclical, gradual increase).

Examples:

- For a cyclical workload that has a steady requirement throughout the year but peaks at the end of every quarter, the estimate should factor for the minimum fixed capacity for the year and the expected peak capacity only for a few days every quarter.
- For dev & test environments that are expected to be up and running only during business hours in the day and for limited duration in the project, costing estimates should factor only for the total expected hours across the project duration instead of the entire period.

As in case of traditional budgeting, the department must factor for any security services, migration and cloud managed services, support services costing over and above the cloud services' costing. CSPs offer transparent public pricing and pricing calculators that can be used for budgetary estimations.

2. Re-thinking General Requirements

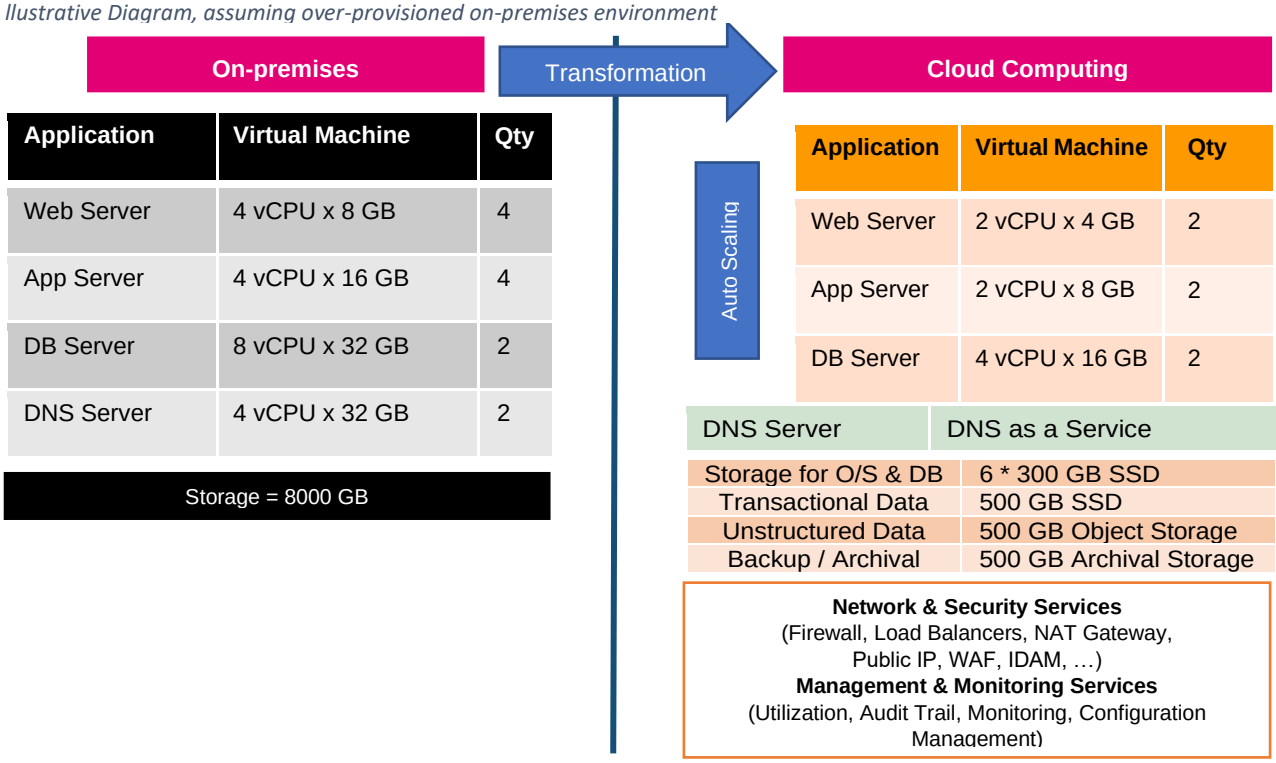
Typically, departments come across two major scenarios –

i. Lift and Shift (migrate / deploy an existing application into cloud)
ii. New Solution (develop a new application on cloud).

i. Lift-and-Shift Scenario

Considering that typical on-premises (or a co-location facility like SDC) infrastructure is under-utilized, departments should assess their current capacity utilizations (e.g., CPU / Memory Utilization; Storage Capacity Utilization; IOPS requirements) and frame the requirements for cloud taking current utilizations into consideration.

Illustrative Diagram, assuming over-provisioned on-premises environment



Requirements in cloud should be defined following the principles of agility and elasticity	
1	Do not plan for peak capacity upfront.
2	Start with smaller configuration instances and Right size[14] instances based on current utilizations.
3	Leverage the expertise of Cloud Service Providers for workload assessments to help define requirements. It is a common practice and the assessment is considered a business development cost by CSPs.
4	Start with fewer instances and avail Auto-scaling Feature
5	Identify the pre-production environments and factor only for the time that they are expected to be running
6	Right size storage and start with smaller storage capacity; Use the appropriate storage service based on the requirement – SSD, HDD, Object Storage, Archival and Deep Archival.
7	Leverage platform services (e.g., Load Balancer, API Gateway, DNS Service) where available that can eliminate the need to factor for compute, storage, software separately.
8	Include services beyond compute and storage to discover the total cost of deployment. For example: security, networking, monitoring & management

[14] **Right Size:** Optimize resource allocation based on expected usage

ii. Procurement for New Solutions (develop a new application on cloud).

In scenarios, where the service provider / application developer is responsible for developing the application as well as hosting, the solutioning should be left to the bidders. The cloud requirements should not be prescriptive and cloud services should not be limited to compute and storage so that the bidders are able to architect using modern application design principles (e.g., micro-services architecture) leveraging breadth of cloud services to design and propose a cost optimal solution.

The department should only provide the performance based / outcome requirements. The service provider should get the flexibility to architect using the breadth of cloud services and quote with their best fit services and cost optimal solution.

3. Rethinking Network and Security Requirements

Department should define their security requirements (e.g., Firewall, Encryption, HSM[15]) to secure the applications in cloud as they would in a traditional on-premises environment.
Departments can also use additional third-party security tools (e.g., Data Leak Protection, Next Generation Firewall, Advanced Threat Analytics, Vulnerability & Penetration Testing) where relevant to complement and enhance operations in the Cloud. Key difference in cloud would be to define these requirements as services.

For example, Load Balancer requirements should be defined in terms of number of connections, data processed as against the traditional appliance-based requirements.

Departments should ensure that the CSPs comply to the required security certifications mentioned in Section 3.3, and are audited by STQC.

4. Re-thinking Business Continuity and DR Requirements

Business continuity and Disaster Recovery planning focuses on continuity of services during and after a disruption (e.g., hardware, software, physical disruption).

Traditionally, Disaster Recovery involves off-site duplication of data and infrastructure, deployment on Active-Passive[16] model and conducting DR drills at regular intervals. However, because of the additional costs of procuring and maintaining *idle infrastructure*, associated license costs (that may never be used during the course of the project) and connectivity between the two locations, departments tend to avoid setting up DR environments. Even when a DR is setup, the service levels, in case of a DR event, are impacted because of provisioning of less than 100% of infrastructure in the DR.

Cloud, eliminates the need for duplicate provisioning of compute resources. The fully provisioned recovery environment is only launched during a disaster and thus significantly reduces the cost for disaster recovery. Moreover, some of the CSPs offer

[15] **HSM**: A hardware security module (HSM) is a physical computing device that safeguards and manages digital keys, performs encryption and decryption functions for digital signatures, strong authentication and other cryptographic functions
[16] **Active- Passive:** The **passive** (a.k.a. failover) server serves as a backup that's ready to take over as soon as the **active** (a.k.a. primary) server gets disconnected or is unable to serve (Ref: Jscape)

an ability, without any additional cost implications, to deploy production applications across physically distinct data center facilities in an [17]Active-Active mode, where data is synchronously replicated across both locations and both the data center facilities are active and handling requests. In case of any failure of one of the facilities, the requests will be automatically directed to and served by the second facility. This provides the ability to maintain business continuity / DR without incurring additional costs.

5. Defining Scope of Work: MSP and CSP

Case 1: Department has an in-house IT team or a Service Provider already contracted (existing contract has either the scope of migration and managed services included or flexibility to include as a change request)

- The scope of work for procurement would be limited to cloud services and procured either directly from the CSP or one of their authorized partners.

Case 2: Department does not have the in-house expertise

- The department may need to include migration and cloud managed services under the scope of work and procure the same from the CSP or one of their Managed Service Partners (MSP).
- The department should have read-only access to the cloud console[18] that gives the department (or their nominated agencies) a complete view into the provisioned cloud services and their configurations, utilization and other reports.

6. Evaluating as a Service

Cloud is a commercial service offering that is offered as a Service with standard service levels. Unlike traditional infrastructure procurement, departments should frame the evaluation criteria via which they can evaluate cloud services across different cloud service providers.
Some of the parameters that may be used for evaluating cloud are:

Breadth of services	e.g., support to different operating systems & databases, cost optimization services, automated compliance checks, security services
Depth of services	e.g., extent of automation available, nature of self-service
Quality of services	e.g., uptime service levels for compute, storage
Proof of Capability (POC)	Demonstration of the cloud services through the cloud console
QCBS	Quality and Cost Based Selection

7. Re-thinking Commercial Evaluation

As against the traditional model of defining fixed configurations & capacities, discovering fixed unit prices, commercial evaluation for cloud has to be re-framed so

[17] An **active-active** model is typically made up of at least two nodes, both actively running the same kind of service simultaneously. (Ref: Jscape)
[18] **Cloud Console:** A user interface to manage all cloud services and configuration.

that the service provider is able to take advantage of the breadth of services during the course of contract.

The commercial evaluation framework should consider the following commercial characteristics of cloud technologies:

- Dynamic and transparent public pricing
- Multiple pricing models (e.g., on-demand, committed)
- Volume-based discounting.

This helps department take advantage of continuous price reductions by the CSP, access multiple discounting models to optimize the overall cloud consumption and any innovations during the project.

i. <u>For lift-and-shift migrations</u>

- Adopt a **scenario-based** Total Cost of Ownership (TCO) evaluation approach, where the department evaluates prices for multiple pricing models(e.g., on-demand, committed) and a variety of services that may be required such as compute, storage, network, security, management & monitoring services. This approach allows for agility to optimize the project.

- This **scenario-based** approach leads to evaluating on overall cumulative commercials that will be higher than the estimated cost of the project. Since the payment will be on a variable OpEx model, **the total calculated for commercial evaluation is not any indication of the payment obligations** from the department to the selected service provider.

	Service Type	**Instance**	**Planned Duration**	**Quantity**	**Unit Discovered Price per hour**	**Amount** (Summation as if all the services are being used for the planned duration, which would never actually be the case)
Vendor 1 (L1)	Web Server	4 vCPU x 8 GB - on-demand	3	2	X	Y
	Web Server	4 vCPU x 8 GB - Reserved	12	2	X	Y
	Web Server	2 vCPU x 4 GB - On demand	3	2	X	Y
	Web Server	2 vCPU x 4 GB - Reserved	12	2	X	Y
	Web Server	4 vCPU x 16 GB - On demand	12	2	X	Y
	App Server	4 vCPU x 32 GB	12	2	X	Y
	DB Server	8 vCPU x 32 GB	12	2	X	Y
	Price discovered for all above services for the purpose of commercial evaluation of vendors and selection of L1. This is **NOT** a contract value and the department won't have to pay this amount.					**Total = Y1**
Vendor 2						**Y2**
Vendor 3						Y3

Disclaimer: this table is only for illustration purposes and numbers are hypothetical.

- The following should be explicitly mentioned during the procurement:
  - Requirements presented as part of Financial Proposal is for price discovery and evaluation purpose only and will not infer any commercial commitment to the Bidder.

- Payment will be based on consumption of cloud services - the actual usage measured - and as per the “Unit Costs” under Pricing Summary Sheet

For new solution procurement,

Where the service provider / application developer is responsible for developing the application as well as hosting and the solutioning is left to the bidders, the department should **avoid scenario-based pricing.**

Since different providers are likely to offer different architectures / services, department should evaluate on the end to end Total Cost of Ownership (TCO) for the solution. The commercial evaluation should discover and evaluate on the overall cost of implementation & hosting the solution.

8. Re-thinking Contracting

Unlike traditional fixed bill of quantity and fixed price contracting, the clauses for cloud contracting must be designed with the following key principles:

i. Lift-and-shift procurement scenario:

Where the department is procuring only cloud and/or managed services (and not a turnkey procurement that includes solution):

- *Overall Value (TCO) used for arriving at the L1 / Best Value Provider becomes an estimated contract value (maximum value of contract). Estimated contract value after commercial evaluation, is not a commitment of payment to the Service Provider.*
- Embrace dynamic and public pricing including access to CSP’s price reductions
- Optimize and consume from the breadth of cloud services within the maximum value of contract
- Ability to apply multiple discounting models during the contract
- *Variable OpEx Payments*:
  i. Paying for the resources that are consumed in the payment period.
  ii. The contract value is only an estimated maximum of cumulative payments. Actual payments may range from 0% (in case of no provisioning of resources) to 100% of the contract value.
  - **Invoicing:** Factor for variable OpEx payments each month. The invoice should enclose the following:
    - Detailed usage report providing details of the consumption.
    - Detailed resource utilization report
    - SLA measurement report

- Department can continue to consume services (even beyond the original contract duration) if the cumulative payments don't exceed the maximum value of contract.

<u>For both lift-and-shift and new solution procurement scenarios:</u>

- Leverage CSP's standard SLAs (e.g., uptime, durability) as against traditional datacenter SLAs.
- *Ownership of Data in Cloud:*
  The ownership of the *Customer Content*[19] stored in Cloud shall be with the purchaser/user department. For example, *Customer Content* includes Content that Customer or any End User stores in Cloud.
- *Audit rights of the provisioned cloud services through the cloud console:*
  CSP must provide access to the cloud management console to the Purchaser or the auditor to be able to review all of the provisioned services required for audit.
- Exit Management and Transition-Out:

A major benefit of cloud computing is the flexibility to avoid traditional vendor lock-in. Cloud customers are not buying physical assets, and CSPs are required to provide easy portability. Departments should consider the availability of technical standards for cloud interfaces which reduce the risk of vendor lock-in.

A process needs to be defined during procurement to account for the need to transition the whole system to another cloud service provider in the future. The following considerations are important:

a) Visibility and ownership of data and critical assets with department.

b) Mandatorily enable audit trail, flow logs and transfer all logs to Government / Replacement Provider.

c) In case of a contract with an MSP, visibility of any 3rd party contracts (e.g., software OEMs, CSP) and provision to transfer / assign the same to Government in case of exit of the current operator.

d) In case of a contract with CSP, availability of services and rights transfer Customer Content to a different environment (on-premises or another cloud provider). CSP should allow Government to retrieve / transfer customer content hosted with the CSP.

e) In case of a contract with MSP, defined exit management process and support from the incumbent managed service provider to transition the customer content & operations to Government / Replacement Provider in case a transition is required.

[19] "Customer Content" means Content that Purchaser or any End User transfers to IA for processing, storage or hosting in relation to the Services and any computational results that the Purchaser or any End User derive from the foregoing through its use of the Services

4.3. Governance and Continuous Optimization

Governance in Cloud

If departments do not have in-house capacity to migrate to cloud or manage the provisioned environment, they can opt for MSPs(managed service providers) who provide the handholding support to the government departments in migrating to cloud and other managed services. The departments may procure cloud and managed services from an authorized partner (Managed Service Provider) of the CSP.

However, even with a MSP in place, in view of the shared responsibility and pay-as-you-go model, it is essential that the Department monitors the operational activities to have the complete view into the provisioned cloud services and their configurations. CSPs offer built-in cloud features that provide Departments with visibility into data, performance, and resource usage. The services can help departments gain more insight into their cloud operations, giving the means to better control their security and providing information for data-driven decisions. Using these features the department must:

- Review and validate the security configurations
- Review the notifications and patches released by the CSP and validate that they are being used
- Confirm that the audit trails (e.g., who is accessing the services, changes to the configurations, etc.) are captured for supporting any downstream audits of the projects by the finance or audit organization.
- Department also needs to have the visibility into the provisioned infrastructure (including the utilizations) so that there is no over-provisioning leading to excess payments to the MSP.

Optimization

Good governance of cloud achieves optimization. Most CSPs provide advisory tools for various operational needs like establishing new workflows and developing applications, based on evolving best practices. They also make recommendations for on-going improvements. It is necessary that the department takes advantage of these recommendations on a regular basis to help keep their solutions provisioned optimally.

While CSPs provide governance tools and recommendations, they don't have a direct incentive to save costs for the department. Therefore, the department must proactively understand the latest recommendations to significantly bring down their own costs. For example, the latest series of processors for the same configuration can bring down cost by almost half. Since license cost is a function of number of CPUs, compute optimization also brings down License costs.

5. Pillar D: Cloud Adoption Support

Cloud is the future, and the quicker we adopt the better. ITE&C Department understands that there would be a broad range of challenges – ranging from new responsibilities, upskilling of department's technical team, new payment models, and many more. To facilitate a smooth transition, ITE&C Department will offer proactive support.

However, the departments must nominate a resource to work on cloud. The resource should attend the cloud workshops organized by ITE&C Department.

5.1. Cloud Centre of Excellence

ITE&C Department is setting up a dedicated team of cloud specialists to accelerate cloud adoption across Telangana's user departments by propagating best practices and capacity building across functions.

The key function of the Cloud Centre of Excellence would be:

- Assist user departments to comply with Telangana's cloud mandate.
- Conduct a series of capacity building sessions for all key stakeholders (including procurement, legal, budget/finance, security, IT, and business leadership) to help those with institutional knowledge understand the cloud.
- Provide advisory services for budgeting, evaluation, procurement (contracting, payment mechanisms, SLAs etc.) governance and continuous optimization.
- Provide advisory services– migration plan, to-be architecture, network & security configurations, etc.

5.2. Catalogue of CSP services

Going forward, to further simplify the procurement process and accelerate cloud adoption, a catalogue of CSP's services along with their discovered prices, would be made available on the e-procurement portal of Telangana State Technology Services (TSTS).